INTELLIGENCE COMMUNITY STANDARD NUMBER 705-2

STANDARDS FOR THE ACCREDITATION AND RECIPROCAL USE OF SENSITIVE COMPARTMENTED INFORMATION FACILITIES (EFFECTIVE: 11 FEBRUARY 2013)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; Executive Order 13526; Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities*; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Standard sets forth the criteria that apply to the accreditation of sensitive compartmented information facilities (SCIF) to enable reciprocal use by all Intelligence Community (IC) elements and to facilitate information sharing to the greatest extent possible.

C. APPLICABILITY: This Standard applies to the IC, as defined by the National Security Act of 1947, as amended, and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

D. ACCREDITATION

1. Accreditation is the beginning of a life-cycle process of continuous monitoring and evaluation, periodic re-evaluations and documentation reviews to ensure the SCIF is maintained in an accredited state. To ensure proper implementation of these standards, the National Counterintelligence Executive (NCIX) may conduct assessments of SCIFs in coordination with Accrediting Officials (AO) and Cognizant Security Authorities (CSA).

a. A letter of accreditation is a formal statement on behalf of the IC element head that a facility has been designed, constructed, inspected, and certified for the protection of all Sensitive Compartmented Information (SCI) compartments, programs or special activities in accordance with the provisions of ICD 705. Letters of accreditation shall include:

(1) SCIF Identity (number and or location)

(2) SCIF Type (e.g., open storage, closed storage)

(1) Acoustic requirements (e.g., discussion or non-discussion, amplified or non-amplified);

(2) Effective date of accreditation;

(3) Statement that SCIF meets all physical and technical security standards; and

(4) Waivers that were approved, to include details of the standard not met and when it is scheduled to be met or standard(s) exceeded.

2. Accreditation Process

a. SCIF inspections and evaluations shall be performed by the AO, or designee, prior to initial accreditation. The accreditation process shall include a review of documents relating to SCIF design, construction and operations. Documents shall include, but not be limited to:

(1) Fixed facility checklists;

(2) Standard operating procedures;

(3) Emergency plans;

(4) Construction Security Plan; and

(5) Waiver request packages and supporting documentation, if applicable.

b. A TEMPEST review and evaluation shall be included in the accreditation documentation. TEMPEST review and verification of countermeasures by the appropriate Certified Technical TEMPEST Authority is a necessary part of the accreditation process.

c. When deemed necessary by the AO, a technical surveillance countermeasures (TSCM) inspection may be required for a new SCIF or significant SCIF renovation.

3. Evaluations. The CSA shall ensure that regular, periodic re-evaluations are conducted to ensure continued security of the SCIF based on the sensitivity of programs, threat, facility modifications, and past security performance.

4. Re-accreditation

a. SCIFs that have waivers issued under previous standards shall be reviewed based upon the most current standards in accordance with guidance issued by the NCIX.

b. All SCIFs shall be re-accredited using current standards when there are major modifications to the SCIF, or changes to the sensitivity of programs or to the threat.

c. SCIFs that have been de-accredited and controlled at the Secret level for less than one year may be re-accredited once based upon the standards used for the original accreditation and a review of an updated facility accreditation package and inspection.

d. CSAs shall ensure that the results of all SCIF re-accreditations are reported to the NCIX via the SCIF Repository within 30 days of the evaluation completion.

5. De-accreditation

a. The de-accreditation of a SCIF is a formal notification to the DNI (via the SCIF Repository) that the facility is no longer accredited.

b. The AO shall refer to the *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (hereinafter "*IC Tech Spec*") for procedures to sanitize facilities and ensure that SCI and observable elements of the mission's operation once contained within the SCIF are properly removed, disposed of and that nothing is left behind.

c. The *IC Tech Spec* shall provide a list of the minimum actions to be taken when a facility is de-accredited.

E. Reciprocity

1. Any SCIF that has been accredited by an IC element AO or designee shall be reciprocally accepted for use as accredited by all IC elements when there are no waivers to the requirements established in IC Standard 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities,* and this IC Standard.

2. In SCIFs that are under a co-use agreement a tenant shall accept the SCIF sponsor's accreditation. If modification of the SCIF is required to meet a different type or use (e.g., open storage vs. closed storage or discussion vs. non-discussion), the cost of modifications shall be borne by the tenant that requires the modifications, unless an alternate agreement is reached. In exceptional circumstances where there is a documented mission need to exceed the uniform security requirements established pursuant to ICD 705, an IC element head may grant a waiver, in accordance with ICD 705 and IC Standard 705-1.

3. Reciprocity is a condition that occurs when there is a requirement to share an accredited SCIF or portion thereof with a compartment, program or special activity that is sponsored by an IC element or organization other than the current SCIF Sponsor.

4. Co-use

a. IC elements or organizations desiring to co-use a SCIF shall accept current accreditations when there are no waivers.

b. A co-use agreement shall be coordinated and signed between the proposed tenant's AO or designee and the host AO or designee that outlines the responsibilities of each. A co-use agreement is not required when sharing a SCIF by two or more components under the cognizance of the same IC element. Occupancy by the new tenant may occur before formal co-use approval with the consent of both AO or designees. Co-use agreements shall be coordinated with information system security representatives of both elements.

c. The original host AO shall retain security cognizance of the facility unless agreed upon by all concerned parties and documented within the co-use documentation.

d. SCIFs may temporarily store SCI on behalf of other organizations for up to seven days for any SCI compartment, sub-compartment or program; specific storage requirements may be necessary for some program information. Storage requirements exceeding seven days require a formal co-use agreement.

e. The SCIF security officer may allow conference rooms within a SCIF under their cognizance to be used on an occasional basis by other organizations to hold SCI discussions not related to the CSA without seeking a co-use agreement. CSAs shall be notified within 10 days when this occurs.

5. Prevention of unauthorized access to additional SCI compartments within a shared SCIF.

a. In circumstances where a SCIF is under a co-use agreement and/or personnel are not briefed to all of the respective programs, procedures shall be instituted by the stakeholder CSAs to prevent unauthorized physical access to that specific compartment, sub-compartment or program information (hereinafter "compartmented information"). Physical and visual access to the compartmented information by unauthorized personnel shall be controlled by partitions, procedures, visual recognition or mechanical/electronic access control devices that shall be specified and approved by the stakeholder CSAs. See the *IC Tech Spec* for details.

b. Additional security measures (e.g., separate reading room) used to further isolate controlled access program information will require the IC element head to report this condition through the Assistant Director of National Intelligence for Policy, Plans, and Requirements to the DNI at the time of establishment and annually thereafter to assess compliance with policy and impact to information sharing. The NCIX will use audits and periodic reviews to monitor each element's use of program approved spaces to ensure additional security measures are appropriately implemented.

c. TEMPEST, administrative telephone, and TSCM requirements for the parent SCIF shall apply to the compartmented area.

F. EFFECTIVE DATE: This Standard becomes effective on the date of signature.

National Counterintelligence Executive

2/11/13
Date